REMARKS

Favorable reconsideration of this application is respectfully requested in view of the
amendments above and the following remarks. Claims 1, 3-12, 14-25, 27-30 and 42-44 are
pending of which claims 1, 12, 21 and 42 are independent. Claims 2, 13, 26 and 31-41 are
canceled, and claims 43-44 are new.

Claims 1, 2, 8-13, 20-30 and 42 were rejected under 35 U.S.C. §102(b) as being
anticipated by Goldschlag et al., "Hiding Routing Information"; hereinafter referred to as
Goldschlag.

Claims 3-7 and 14-19 were rejected under 35 U.S.C. §103(a) as being unpatentable
over Goldschlag in view of Clark et al.,"Freenet: A Distirbuted Anonymous INformation
Storage and Retrieval System", hereinafter referred to as Clarke.

These rejections are respectfully traversed for the reasons set forth below.

Drawings

The Applicants thank the Examiner for indicating that the drawings filed on February
8, 2002, have been accepted.

Claim Rejections Under 35 U.S.C. §102(b)

The test for determining if a reference anticipates a claim, for purposes of a rejection
under 35 U.S.C. § 102, is whether the reference discloses all the elements of the claimed
combination, or the mechanical equivalents thereof functioning in substantially the same way
to produce substantially the same results. As noted by the Court of Appeals for the Federal
Circuit in *Lindemann Maschinenfabrick GmbH v. American Hoist and Derrick Co.*, 221

12

PATENT

HP Docket No.: 100200290-1
App. Serial No. 10/084,499

USPQ 481, 485 (Fed. Cir. 1984), in evaluating the sufficiency of an anticipation rejection

under 35 U.S.C. § 102, the Court stated:

> Anticipation requires the presence in a single prior art reference
> disclosure of each and every element of the claimed invention,
> arranged as in the claim.

Therefore, if the cited reference does not disclose each and every element of the claimed

invention, then the cited reference fails to anticipate the claimed invention and, thus, the

claimed invention is distinguishable over the cited reference.

Claims 1, 2, 8-13, 20-30 and 42 were rejected under 35 U.S.C. §102(b) as being

anticipated by Goldschlag.

Claim 1 has been amended to include the features of claim 2. Claim 1 recites:

> retrieving an identity of said next peer according to said path
> for said information and a respective index peer of said next peer;
> encrypting said path index with a public key of said respective
> index peer of said next peer to form a next state of said path index; and
> transmitting a new message with said information and said next
> state of said path index as said path index to said next peer.

Goldschlag fails to teach an index peer of a next peer, retrieving an identity of a next

peer using a respective index peer of the next peer, and encrypting the path index with public

key of the index peer of the next peer.

Goldschlag discloses encrypting an onion with a public key of a next peer but fails to

teach encrypting the onion with a public key of an index peer of the next peer. In particular,

Goldschlag discloses a forward onion in figure 2. The onion is a data structure composed of

layer upon layer of encryption wrapped around a payload. The basic structure of the onion is

based on the route to the responder that is chosen by the initiator's proxy.

13

PATENT   HP Docket No.: 100200290-1
                                              App. Serial No. 10/084,499

Goldschlag discloses that the data structure of an onion received at a node Px looks

like this:

   {*exp time, next hop, Ff, Kf, Fb, Kb,* payload}PKx

Here PK is a public encryption key for routing node P, who is assumed to have the

corresponding decryption key. The onion appears to be encrypted with the public encryption

key of the next node, such as PKx. An index peer for a next node is not disclosed in

Goldschlag and using a public key of an index node for a next peer is not disclosed in

Goldshclag.

Goldschlag discloses that the two function key pairs, *i.e., Ff, Kf, Fb, Kb,* specify the

cryptographic operations and keys to be applied to data that will be sent along the virtual

circuit. Use of the functions keys for encrypting data is further described in section 4

"Implementation" in Goldschlag. After using the "create" command to establish virtual

circuit, the "data" command is used to pass a stream of data from the initiator to the

responder. The initiator node breaks the data stream into payload sized chunks, and

repeatedly pre-crypts each chunk of the data stream using the inverse of the cryptographic

operations specified in the onion, innermost first. At a node receiving the onion, the

function/key pairs that are applied, and the virtual circuit identifier of the connection to the

next node are obtained from a table. The cryptographic function key pair associated with the

circuit (for the appropriate direction) and the virtual circuit identifier of the connection to the

next node is obtained. It then peels off a layer of cryptography and forwards the peeled

payload to the next node.

Thus, Goldschlag discloses encrypting payload data of the data stream with the

function key pairs. However, the virtual circuit identifier in Goldschlag is not encrypted with

the function key pairs or a public key of an index peer of a next peer. Accordingly, claims 1

14

HP Docket No.: 100200290-1
                                              App. Serial No. 10/084,499

and 3-11 are believed to be allowable. Also, claim 11 is directed to an index entry including

respective index peers, which is not taught by Goldschlag.

Independent claim 12 has been amended to include the features of dependent claim

13. Claim 12 recites, "forming a next state of said path index by encrypting said path index

with a public key of a respective index peer of said next peer." Goldschlag fails to teach this

feature for the reasons stated above. Accordingly, claims 12 and 14-20 are believed to be

allowable.

Claim 21 has been amended to include the features of claim 26. Claim 21 recites:

> generating an encryption key;
>
> encrypting said encryption key with a public key of said
> requestor;
>
> encrypting said encryption key with a public key of said
> provider; and
>
> encrypting a transaction identifier, a reference for said
> information, and a first next peer according to said path with said encryption
> key.

As described above, Goldschlag discloses that the two function key pairs, *i.e., Ff, Kf,*

Fb, Kb, specify the cryptographic operations and keys to be applied to data that will be sent

along the virtual circuit. However, Goldschlag fails to teach the two function key pairs are

used to encrypt a transaction identifier, a reference for said information, and a first next peer

according to said path with said encryption key. Accordingly, claims 21-25 and 27-30 are

believed to be allowable.

Claim 42 recites:

15

if a label stored at the intermediate peer matches the predetermined label, the intermediate peer retrieves a previously stored message and generates a next state of the predetermined label for the setup message.

Goldschlag discloses a create message in section 4 "Implementation" used to create the virtual circuit. However, Goldschlag fails to teach or suggest retrieving a previously stored message if there is a match between a received label in a set-up message and a stored label and generating a next state of the predetermined label for the setup message if there is a match. Accordingly, claims 42-44 are believed to be allowable.

Claim Rejections Under 35 U.S.C. §103(a)

The test for determining if a claim is rendered obvious by one or more references for purposes of a rejection under 35 U.S.C. § 103 is set forth in MPEP § 706.02(j):

> To establish a *prima facie* case of obviousness, three basic criteria must be met. First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, the prior art reference (or references when combined) must teach or suggest all the claim limitations. The teaching or suggestion to make the claimed combination and the reasonable expectation of success must both be found in the prior art and not based on applicant's disclosure. *In re Vaeck*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991).

Therefore, if the above-identified criteria are not met, then the cited reference(s) fails to render obvious the claimed invention and, thus, the claimed invention is distinguishable over the cited reference(s).

Claims 3-7 and 14-19 were rejected under 35 U.S.C. §103(a) as being unpatentable over Goldschlag in view of Clark.

16

Clark discloses a system where each node in a peer-to-peer network maintains its own data store. Hash tables are used to determine where to send a request. A key and a hops-to-live value are specified in a request. A node receiving the request determines whether it stores the requested data. If not, the receiving node looks up the nearest key in its routing table and forwards the request to the corresponding node. If the data is found at a node receiving the request, the data is sent back to the requestor. If Clarke is combined with Goldschlag, each node in the peer-to-peer network would have to know a path between itself and a requestor to provide the Onion routing of Goldschlag. This is unlikely in a large peer-to-peer network, and furthermore would waste valuable data storage space. According to an embodiment of the Applicants' system, a directory 130 shown in figure 1, such as trusted node, determines paths for requests and transmits a set-up message to all the nodes in the path. In this embodiment, each node in the system 100 does not need to know of other peers that can form a path between a provider and a requestor, because the directory 130 stores that information. Neither Clarke nor Goldschlag discloses a peer similar to the directory 130. Thus, there is unreasonable expectation of success when combining the onion routing of Goldschlag with Clarke. Accordingly, a *prima facie* case of obviousness has not been established and the rejection should be withdrawn. Accordingly, claims 3-7 and 14-19 are believed to be allowable.

Newly Added Claims

Claims 43 and 44 are new. Claim 43 recites, "encrypting the received predetermined label with a public key of a respective index peer of the next peer." Claim 44 recites that the stored message comprises "an encryption key encrypted with the public key of the requestor."

PATENT   HP Docket No.: 100200290-1
                                                    App. Serial No. 10/084,499

These features are not taught or suggested by the prior art of record. Accordingly, claims 43
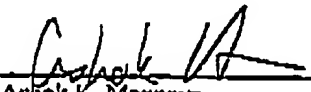and 44 are believed to be allowable.

CONCLUSION

As all of the outstanding rejections have been traversed and all of the claims are
believed to be in condition for allowance, the Applicants respectfully request issuance of a
Notice of Allowability. If the undersigned attorney can assist in any matters regarding
examination of this application, the Examiner is encouraged to call at the number listed
below.

                                              Respectfully submitted,

Date: March 17, 2006   By   _____
                                            Ashok K. Mannava
                                            Registration No. 45,301

                                            MANNAVA & KANG, P.C.
                                            8221 Old Courthouse Road
                                            Suite 104
                                            Vienna, VA 22182
                                            (703) 652-3822
                                            (703) 880-5270 (facsimile)

18